D2293256

CITATION

JACQUELINE HORTON, INDIVIDUALLY AND O/B/O OTHERS SIMILARLY SITUATED	**Tenth Judicial District Court**
VS	**Parish of Natchitoches**
WILLIS KNIGHTON MEDICAL CENTER	**State of Louisiana**
DOCKET NUMBER: C-93767 B	

TO: WILLIS KNIGHTON MEDICAL CENTER
THROUGH ITS DESINATED AGENT FOR SERVICE PROCESS:
LAMAR P. PUGH
333 TEXAS STREET
SHREVEPORT, LA 71101

YOU HAVE BEEN SUED.
Attached to this Citation is a certified copy of the Petition. The petition tells you what you are being sued for.

You must EITHER do what the petition asks, OR, within TWENTY-ONE (21) days after you have received these documents, you must file an answer or other legal pleadings in the Office of the Clerk of this Court at the Natchitoches Parish Courthouse, in the City of Natchitoches in said Parish.

If you do not do what the petition asks, or if you do not file an answer or legal pleading within TWENTY-ONE (21) days, judgment may be entered against you without further notice.

Witness the Honorable Judges of our said Court on this JANUARY 30, 2023.

DAVID STAMEY, Clerk of Court

BY: Danielle B. Green
Deputy Clerk
Natchitoches Parish

ATTORNEY:
KEENAN K. KELLY

ATTACHMENTS:
CERTIFIED COPY OF PETITION FOR DAMAGES (CLASS ACTION), PLAINTIFF'S FIRST SET OF INTERROGATORIES, AND REQUEST FOR PRODUCTION OF DOCUMENTS

NOTICE

Access to the Natchitoches Parish Courthouse is available to those persons with disabilities who require a ground level entrance through the St. Denis Street entrance. To request special accommodation call the Clerk of Court at (318) 352-8152 or the office of the Chief Judge at (318) 357-2210. The following facilities are available to persons with disabilities:

*Ground level access at St. Denis Street entrance to courthouse
*Handicapped accessible elevator to all floors
*Wheelchair accessible doors to courtrooms

JACQUELINE HORTON, individually and on behalf of others similarly situated,

NUMBER: 93767-B

TENTH JUDICIAL DISTRICT COURT

v.

NATCHTOCHES PARISH, LOUISIANA

WILLIS-KNIGHTON MEDICAL CENTER

PETITION FOR DAMAGES

CLASS ACTION

Plaintiff, Jacqueline Horton, individually and on behalf of all other current Louisiana citizens similarly situated, brings this suit against Defendant, Willis-Knighton Medical Center, d/b/a Willis-Knighton Health System ("Willis-Knighton") , and respectfully represents as follows:

INTRODUCTION

1.

This case arises from Defendants' systematic violation of the medical privacy rights of its customers, exposing highly sensitive personal information to third parties without their knowledge or consent.

2.

As part of its Notice of Privacy Practices, Defendant touts that it is "committed to protecting your medical information" and explains that it is "required by law to ensure the privacy of your identifiable medical information explains." Defendant further promises that "We will not use and disclose your Protected Health Information for marketing purposes without your written authorization." Contrary to these assurances, Defendant does not follow this policy, nor the law prohibiting such disclosures.

3.

At all relevant times, Defendants disclosed information about their customers – including their status as patients (and/or potential patients), their physicians, their medical treatments, the hospitals they visited, and their personal identities – to Facebook (and/or other third parties) without their knowledge, authorization, or consent.

4.

Defendants disclosed this protected health information through the deployment of various digital marketing and automatic re-routing tools embedded on its websites that purposefully and

intentionally re-direct customers (and/or would-be customers') personal health information to third parties who exploit that information for advertising purposes. Defendants' use of these re-routing tools causes their patients' personally identifiable information and the contents of its patients' communications exchanged with Defendants to be automatically re-directed to third parties in violation of those patients' reasonable expectations of privacy, their rights as patients, their rights as citizens of the State of Louisiana, and both the express and implied promises of Defendants.

5.

Defendants' conduct in disclosing such protected health information to Facebook and/or other third parties violates Louisiana law, including La. R.S. 15:1303 (Interception and Disclosure of Wire, Electronic, or Oral Communications), La. R.S. 51:3074 (Protection of Personal Information; Disclosure upon Breach in the Security of Personal Information; and Notification Requirements), 48 La. Admin. Code Pt. 1, §9319 (Patient Rights and Privacy), and La. Admin. Code Pt. 1, §505 (Confidentiality and Disclosure), as well as Louisiana Civil Code Articles 2315, 2316 and/or 2324(A).

6.

On behalf of herself and all similarly situated citizens of Louisiana, Plaintiff seeks an order enjoining Defendants from further unauthorized disclosures of her personal information; awarding liquidated damages in the amount of $1,000 per violation, attorney's fees and costs; and granting any other relief the Court deems appropriate.

PARTIES TO THE ACTION

7.

Defendant Willis-Knighton Medical Center (d/b/a Willis Knighton Health System)[1] is a Louisiana corporation with its principal place of business located in the Parish of Caddo, at 2600 Greenwood Rd, Shreveport, LA 71103. Defendant is the parent company for multiple healthcare facilities in Louisiana, including Willis-Knighton Medical Center, Willis-Knighton South & Center for Women's Health, WK Bossier Health Center, WK Pierremont Health Center, and a network of other facilities through the Northwest Louisiana area (collectively "WK Health System").[2]

[1] Willis-Knighton Medical Center is the entity name of Willis-Knighton Health System which includes numerous healthcare facilities, including one hospital location also named Willis-Knighton Medical Center. For clarity, references to "Defendant" in this Petition includes the entire Willis-Knighton Health System.

[2] *See, e.g.*, https://www.wkhs.com/locations

8.

Plaintiff, Jacqueline Horton, is an individual domiciled and residing in the Parish of Natchitoches, State of Louisiana. Plaintiff has been treated by Willis-Knighton physicians as a patient and has inquired about treatment by Willis-Knighton as a prospective patient.

JURISDICTION AND VENUE

9.

This Court has personal jurisdiction over Defendant because it regularly conducts business within the State of Louisiana. Indeed, Defendant's principal place of business is located within the State of Louisiana.

10.

Venue is appropriate in this Court because Plaintiff is domiciled and residing in the Parish of Natchitoches, Plaintiff's communications at issue with Defendant occurred in the Parish of Natchitoches, and Defendant's wrongful conduct giving rise to this action occurred and caused Plaintiff injury in the Parish of Natchitoches.

FACTUAL BACKGROUND

A. Willis-Knighton routinely discloses the protected health information of its customers to third parties including Facebook.

11.

Plaintiff is a customer of Willis-Knighton who has received treatment at Willis-Knighton Medical Center.

12.

Under Louisiana Law, all patients have "the right to have his/her medical records, including all computerized medical information, kept confidential." 48 La. Admin. Code Pt. 1, §9319.

13.

Medical patients in Louisiana such as Plaintiff have a legal interest in preserving the confidentiality of their communications with healthcare providers and have reasonable expectations of privacy that their personally identifiable information and communications will not be disclosed to third parties by Defendant without their express written consent and authorization.

14.

As a health care provider, Defendant has fiduciary, common law, and statutory duties to protect the confidentiality of patient information and communications.

15.

Defendant expressly and impliedly promises patients that it will maintain and protect the confidentiality of personally identifiable patient information and communications.

16.

Defendant operates https://www.wkhs.com/ as its primary website for patients.

17.

Defendant's websites are designed for interactive communication with potential customers and patients, including scheduling appointments, searching for physicians, paying bills, requesting medical records, learning about medical issues treatment options, and joining support groups.

18.

Notwithstanding patients' reasonable expectations of privacy, Defendant's legal duties of confidentiality, and Defendant's express promises to the contrary, Defendant disclosed the contents of patients' communications and protected healthcare information *via* automatic re-routing mechanisms embedded in the websites operated by Defendant without its patients' knowledge, authorization, or consent.

B. The nature of Defendant's unauthorized disclosure of customers' health care information.

19.

Defendant's disclosure of personal healthcare information occurred because Defendant intentionally deployed source code on the websites it operates, including www.wkhs.com, that caused patients' personally identifiable information (as well as the exact contents of their communications) to be transmitted to third parties.

20.

By design, Facebook receives and records the exact contents of an existing or potential customer's communications before the full response from Defendant to patients has been rendered on the screen of the customer's computer device and while the communication between Defendant and the potential patient or patient remains ongoing.

21.

Websites like those maintained by Defendants are hosted by a computer server through which the business in charge of the website exchanges and communicates with internet users *via* their web browsers.

22.

The basic command that web browsers use to exchange data and user communications is called a GET request.[3] For example, when a patient types "heart failure treatment" into the search box on Defendants' website and hits 'Enter', the patient's web browser makes a connection with the server for Defendants' website and sends the following request: "GET search/q=heart+failure+treatment."

23.

When a server receives a GET request, the information becomes appended to the next URL (or "Uniform Resource Locator") accessed by the user. For example, if a user enters "respiratory problems" into the query box of a website search engine, and the search engine transmits this information using a GET request method, then the words "respiratory" and "problems" will be appended to the query string at the end of the URL of the webpage showing the search results.

24.

The other basic transmission command utilized by web browsers is POST, which is typically employed when a user enters data into a form on a website and clicks 'Enter' or some other form of submission button. POST sends the data entered in the form to the server hosting the website that the user is visiting.

25.

In response to receiving a GET or POST command, the server for the website with which the user is exchanging information will send a set of instructions to the web browser and command the browser with source code that directs the browser to render the website's responsive communication.

26.

Unbeknownst to most users, however, the website's server may also redirect the user's communications to third parties. Indeed, Google warns website developers and publishers that

[3] *See, e.g.*, https://www.w3schools.com/tags/ref_httpmethods.asp

installing its ad tracking software on webpages employing GET requests will result in users' personally identifiable information being disclosed to Google.[4] Typically, users are provided no notice that these disclosures are being made.

27.

Third parties (such as Facebook and Google) use the information they receive to track user data and communications for marketing purposes.

28.

In many cases, third-party marketing companies acquire the content of user communications through a 1x1 pixel (the smallest dot on a user's screen) called a tracking pixel, a web-bug, or a web beacon. These tracking pixels are tiny and are purposefully camouflaged to remain invisible to users.

29.

Tracking pixels can be placed directly on a web page by a developer, or they can be funneled through a "tag manager" service to make the invisible tracking run more smoothly. A tag manager further obscures the third parties to whom user data is transmitted.

30.

These tracking pixels can collect dozens of data points about individual website users who interact with a website. One of the world's most prevalent tracking pixels, called the Meta Pixel, is provided by Facebook.

31.

A web site developer who chooses to deploy third-party source code, like a tracking pixel, on their website must enter the third-party source code directly onto their website for every third party they wish to send user data and communications. This source code operates invisibly in the background when users visit a site employing such code.

C. Tracking pixels provide third parties with a trove of personally identifying data permitting them to uniquely identify the individuals browsing a website.

32.

Tracking pixels are lines of source code embedded in websites such as Defendant's. Tracking pixels are particularly pernicious because they result in the disclosure of a variety of data that permits third parties to determine the unique personal identities of website visitors. While

[4] https://support.google.com/platformspolicy/answer/6156630?hl=en

most users believe that the internet provides them with anonymity when, for example, they browse a hospital website for treatment information about a medical condition, that is not the case when the hospital website has embedded third party tracking devices, as Defendant has.

33.

For example, an IP address is a number that identifies a computer connected to the internet. IP addresses are used to identify and route communications on the internet. IP addresses of individual users are used by internet service providers, websites, and tracking companies to facilitate and track internet communications and content. IP addresses also offer advertising companies like Facebook a unique and semi-persistent identifier across devices – one that has limited privacy controls.[5]

34.

Because of their uniquely identifying character, IP address are considered protected personally identifiable information. Tracking pixels can (and typically do) collect website visitors' IP addresses.

35.

Likewise, internet cookies also provide personally identifiable information. Cookies are small text files that web servers can place on a user's browser and computer when a user's browser interacts with a website server. Cookies are typically designed to acquire and record an individual internet user's communications and activities on websites and were developed by programmers to aid with online advertising.

36.

Cookies are designed to operate as a means of identification for internet users. Advertising companies like Facebook and Google have developed methods for monetizing and profiting from cookies. These companies use third-party tracking cookies to help them acquire and record user data and communications in order to sell targeted advertising that is customized to a user's personal communications and browsing history. To build individual profiles of internet users, third party advertising companies assign each user a unique (or a set of unique) identifiers to each user.

[5] *See, e.g.*, https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/

37.

Cookies are also considered personal identifiers, and tracking pixels can collect cookies from website visitors.

38.

A third type of personally identifying information is what data companies refer to as a "browser-fingerprint". A browser-fingerprint is information collected about a computing device that can be used to identify the specific device.

39.

These browser-fingerprints can be used to uniquely identify individual users when a computing device's IP address is hidden or cookies are blocked and can provide a wide variety of data. As Google explained, "With fingerprinting, developers have found ways to use tiny bits of information that vary between users, such as what device they have or what fonts they have installed to generate a unique identifier which can then be used to match a user across websites."[6] The value of browser-fingerprinting to advertisers (and trackers who want to monetize aggregated data) is that they can be used to track website users just as cookies do, but it employs much more subtle techniques.[7] Additionally, unlike cookies, users cannot clear their fingerprint and therefore cannot control how their personal information is collected.[8]

40.

In 2017, researchers demonstrated that browser fingerprinting techniques can successfully identify 99.24 percent of all users.[9]

41.

Browser-fingerprints are also considered protected personal identifiers, and tracking pixels can collect browser-fingerprints from website visitors.

42.

A fourth kind of personally identifying information is the unique user identifier (such as Facebook's "Facebook ID") that permits companies like Facebook to quickly and automatically identify the personal identity of its user across the internet whenever the identifier is encountered.

---

[6] *See, e.g.*, https://www.blog.google/products/chrome/building-a-more-private-web/

[7] *See, e.g.*, https://pixelprivacy.com/resources/browser-fingerprinting/

[8] *See, e.g.*, https://www.blog.google/products/chrome/building-a-more-private-web/

[9] *See, e.g.*, https://www.ndss-symposium.org/ndss2017/ndss-2017-programme/cross-browser-fingerprinting-os-and-hardware-level-features/

A Facebook ID is a number string that is connected to a user's Facebook profile.[10] Anyone with access to a user's Facebook ID can locate a user's Facebook profile.[11]

43.

Unique personal identifiers are likewise capable of collection through pixel trackers.

D. Facebook's Business Model: Exploiting Users' Personal Data to Sell Advertising.

44.

Facebook, a social media platform founded in 2004 and today operated by Meta Platforms, Inc., was originally designed as a social networking website for college students.

45.

Facebook describes itself as a "real identity" platform.[12] This means that users are permitted only one account and must share "the name they go by in everyday life."[13] To that end, Facebook requires users to provide their first and last name, along with their birthday, telephone number and/or email address, and gender, when creating an account.[14]

46.

In 2007, realizing the value of having direct access to millions of consumers, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming this service to be a "completely new way of advertising online," that would allow "advertisers to deliver more tailored and relevant ads."[15] Facebook has since evolved into one of the largest advertising companies in the world.[16] Facebook can target users so effectively because it surveils user activity both on and off its website through the use of tracking pixels.[17] This allows Facebook to make inferences about users based on their interests, behavior, and connections.[18]

47.

Today, Facebook provides advertising on its own social media platforms, as well as other websites through its Facebook Audience Network. Facebook has more than 2.9 billion users.[19]

---

[10] *See, e.g.*, https://www.facebook.com/help/211813265517027

[11] *See, e.g.*, https://smallseotools.com/find-facebook-id/

[12] *See, e.g.*, https://www.wsj.com/articles/how-many-users-does-facebook-have-the-company-struggles-to-figure-it-out-11634846701#:~:text=Facebook%20said%20in%20its%20most,of%20them%20than%20developed%20ones.

[13] *See, e.g.*, https://transparency.fb.com/policies/community-standards/account-integrity-and-authentic-identity/

[14] *See, e.g.*, https://www.facebook.com/help/406644739431633

[15] *See, e.g.*, https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/

[16] *See, e.g.*, https://www.pewresearch.org/fact-tank/2021/06/01/facts-about-americans-and-facebook/

[17] *See, e.g.*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[18] *See, e.g.*, https://www.facebook.com/business/ads/ad-targeting

[19] *See, e.g.*, https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

48.

Facebook maintains profiles on users that include users' real names, locations, email addresses, friends, likes, and communications. These profiles are associated with personal identifiers, including IP addresses, cookies, and other device identifiers. Facebook also tracks non-users across the web through its internet marketing products and source code. Facebook also employs algorithms, powered by machine learning tools, to determine what advertisements to show users based on their habits and interests, and utilizes tracking software such as the Meta Pixel to monitor and exploit users' habits and interests.

49.

Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (e.g., age, gender, education, job title, etc.), interests, (e.g., preferred food, movies), connections (e.g., particular events or Facebook pages), and behaviors (e.g., purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

50.

Facebook offers several advertising options based on the type of audience that an advertiser wants to target. Those options include targeting "Core Audiences," "Custom Audiences," "Look Alike Audiences," and even more granulated approaches within audiences called "Detailed Targeting." Each of Facebook's advertising tools allow an advertiser to target users based, among other things, on their personal data, including geographic location, demographics (*e.g.*, age, gender, education, job title, etc.), interests, (*e.g.*, preferred food, movies), connections (*e.g.*, particular events or Facebook pages), and behaviors (*e.g.*, purchases, device usage, and pages visited). This audience can be created by Facebook, the advertiser, or both working in conjunction.

51.

Ad Targeting has been extremely successful due to Facebook's ability to target individuals at a granular level. For example, among many possible target audiences, "Facebook offers advertisers 1.5 million people 'whose activity on Facebook suggests that they're more likely engage with/distribute liberal political content' and nearly seven million Facebook users who

'prefer high-value goods in Mexico.'"[20] Aided by highly granular data used to target specific users, Facebook's advertising segment quickly became Facebook's most successful business unit, with millions of companies and individuals utilizing Facebook's advertising services.

E. Facebook's Meta Pixel tool allows Facebook to track the personal data of individuals across a broad range of third-party websites.

52.

To power its advertising business, Facebook uses a variety of tracking tools to collect data about individuals, which it can then share with advertisers. These tools include software development kits incorporated into third-party applications, its "Like" and "Share" buttons (known as "social plug-ins"), and other methodologies, which it then uses to power its advertising business.

53.

One of Facebook's most powerful tools is called the "Meta Pixel." Once a third-party like Defendant installs the Meta Pixel on its website, by default it begins sending user information to Facebook automatically.[21]

54.

The Meta Pixel is a snippet of code embedded on a third-party website that tracks users' activities as users navigate through a website.[22] Once activated, the Meta Pixel "tracks the people and type of actions they take."[23] Meta Pixel can track and log each page a user visits, what buttons they click, as well as specific information that users input into a website.[24] The Meta Pixel code works by sending Facebook a detailed log of a user's interaction with a website such as clicking on a product or running a search via a query box. The Meta Pixel also captures information such as what content a user views on a website or how far down a web page they scrolled.[25]

55.

When someone visits a third-party website page that includes the Meta Pixel code, the Meta Pixel code is able to replicate and send the user data to Facebook through a separate (but simultaneous) channel in a manner that is undetectable by the user.[26] This information is disclosed to Facebook regardless of whether a user is logged into their Facebook account at the time.

---

[20] *See, e.g.,* https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html

[21] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

[22] *See, e.g.,* https://developers.facebook.com/docs/meta-pixel/

[23] *See, e.g.,* https://www.facebook.com/business/goals/retargeting

[24] *See, e.g.,* https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[25] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector

[26] *See, e.g., In re Facebook, Inc. Internet Tracking Litigation,* 956 F.3d 589, 596 (9th Cir. 2020) (explaining functionality of Facebook software code on third-party websites).

56.

The information Meta Pixel captures and discloses to Facebook includes a referrer header (or "URL"), which includes significant information regarding the user's browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms used to find it.27 When users enter a URL address into their web browser using the 'http' web address format, or click hyperlinks embedded on a web page, they are actually telling their web browsers (the client) which resources to request and where to find them. Thus, the URL provides significant information regarding a user's browsing history, including the identity of the individual internet user and the web server, as well as the name of the web page and the search terms that the user used to find it.

57.

These search terms and the resulting URLs divulge a user's personal interests, queries, and habits on third-party websites operating outside of Facebook's own platform. In this manner, Facebook tracks users browsing histories on third-party websites, and compiles these browsing histories into personal profiles which are sold to advertisers to generate revenue.[28]

58.

For example, if Meta Pixel is incorporated on a shopping website, it may log what searches a user performed, which items of clothing a user clicked on, whether they added an item to their cart, as well as what they purchased. Along with this data, Facebook collects identifying information like IP addresses, Facebook IDs, and other data that allow Facebook to identify the user. All this personally identifying data is available each time the Meta Pixel forwards a user's interactions with a third-party website to Facebook's servers. Once Facebook receives this information, Facebook processes it, analyzes it, and assimilates it into datasets like its Core Audiences and Custom Audiences. Facebook can then sell this information to companies who wish to display advertising for products similar to what the user looked at on the original shopping website.

59.

These communications with Facebook happen silently, without users' knowledge. By default, the transmission of information to Facebook's servers is invisible. Facebook's Meta Pixel

[27] *In re Facebook*, 956 F.3d at 596.
[28] *In re Facebook*, 956 F.3d at 596.

allows third-party websites to capture and send personal information a user provides to match them with Facebook or Instagram profiles, even if they are not logged into Facebook at the time.[29]

60.

In exchange for installing its Meta Pixel, Facebook provides website owners like Defendant with analytics about the ads they've placed on Facebook and Instagram and tools to target people who have visited their website.[30] The Meta Pixel collects data on website visitors regardless of whether they have Facebook or Instagram accounts.[31]

61.

Facebook can then share analytic metrics with the website host, while at the same time sharing the information it collects with third-party advertisers who can then target users based on the information collected and shared by Facebook.

62.

Facebook touted Meta Pixel (which it originally called "Facebook Pixel") as "a new way to report and optimize for conversions, build audiences and get rich insights about how people use your website."[32] According to Facebook, the Meta Pixel is an analytics tool that allows business to measure the effectiveness of their advertising by understanding the actions people take on their websites.[33]

63.

Facebook warns web developers that its Pixel is a personal identifier because it enables Facebook "to match your website visitors to their respective Facebook User accounts."[34]

64.

Facebook recommends that its Meta Pixel code be added to the base code on every website page (including the website's persistent header) to reduce the chance of browsers or code from blocking Pixel's execution and to ensure that visitors will be tracked.[35]

---

[29] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[30] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[31] https://themarkup.org/show-your-work/2022/04/28/how-we-built-a-meta-pixel-inspector
[32] *See, e.g.*, https://developers.facebook.com/ads/blog/post/v2/2015/10/14/announcing-facebook-pixel/
[33] *See, e.g.*, https://www.oviond.com/understanding-the-facebook-pixel
[34] *See, e.g.*, https://developers.facebook.com/docs/meta-pixel/get-started
[35] *See, e.g.*, https://developers.facebook.com/docs/meta-pixel/get-started

65.

Once Meta Pixel is installed on a business's website, the Meta Pixel tracks users as they navigate through the website and logs which pages are visited, which buttons are clicked, the specific information entered in forms (including personal information), as well as "optional values" set by the business website.[36] Meta Pixel tracks this data regardless of whether a user is logged into Facebook.[37] It is unclear how Facebook exploits the data collected from nonusers, but when asked by Congress about Facebook's business practices, Mark Zuckerberg conceded that the company maintains "shadow profiles" on nonusers of Facebook.[38]

66.

For Facebook, the Meta Pixel tool embedded on third-party websites acts as a conduit for information, sending the information it collects to Facebook through scripts running in a user's internet browser, similar to how a "bug" or wiretap can capture audio information.

67.

For example, the Meta Pixel is configured to automatically collect "HTTP Headers" and "Pixel-specific data."[39] HTTP headers collect data including "IP addresses, information about the web browser, page location, document, referrer and person using the website."[40] Pixel-specific data includes such data as the "Pixel ID and the Facebook Cookie."[41]

68.

Meta Pixel takes the information it harvests and sends it to Facebook with personally identifiable information, such as a user's IP address, name, email, phone number, and specific Facebook ID, which identifies an individual's Facebook user account. Anyone who has access to this Facebook ID can use this identifier to quickly and easily locate, access, and view a user's corresponding Facebook profile. Facebook stores this information on its servers, and, in some instances, maintains this information for years.[42]

---

[36] *See, e.g.,* https://developers.facebook.com/docs/meta-pixel/

[37] *See, e.g.,* https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients

[38] https://techcrunch.com/2018/04/11/facebook-shadow-profiles-hearing-lujan-zuckerberg/

[39] *See, e.g.,* https://developers.facebook.com/docs/meta-pixel/

[40] *See, e.g.,* https://developers.facebook.com/docs/meta-pixel/

[41] *See, e.g.,* https://developers.facebook.com/docs/meta-pixel/

[42] *See, e.g.,* https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

69.

Facebook has a number of ways to uniquely identify the individuals whose data is being forwarded from third-party websites through the Meta Pixel.

70.

If a user has a Facebook account, the user data collected is linked to the individual user's Facebook account. For example, if the user is logged into their Facebook account when the user visits a third-party website where the Meta Pixel is installed, many common browsers will attach third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.

71.

Alternatively, Facebook can link the data to a user's Facebook account through the "Facebook Cookie."[43] The Facebook Cookie is a workaround to recent cookie-blocking applications used to prevent websites from tracking users.[44]

72.

Facebook can also link user data to Facebook accounts through identifying information collected through Meta Pixel through what Facebook calls "Advanced Matching." There are two forms of Advanced Matching: manual matching and automatic matching.[45] Manual matching requires the website developer to manually send data to Facebook so that users can be linked to data. Automatic matching allows Meta Pixel to scour the data it receives from third-party websites to search for recognizable fields, including names and email addresses that correspond with users' Facebook accounts.

73.

While the Meta Pixel tool "hashes" personal data—obscuring it through a form of cryptography before sending the data to Facebook—that hashing does not prevent Facebook from using the data.[46] In fact, Facebook explicitly uses the hashed information it gathers to link pixel data to Facebook profiles.[47]

---

[43] *See, e.g.*, https://clearcode.cc/blog/facebook-first-party-cookie-adtech/

[44] *See, e.g.*, https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/

[45] *See, e.g.*, https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[46] *See, e.g.*, https://www.facebook.com/business/help/611774685654668?id=1205376682832142

[47] *See, e.g.*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

74.

Facebook also receives personally identifying information in the form of user's unique IP addresses that stay the same as users visit multiple websites. When browsing a third-party website that has embedded Facebook code, a user's unique IP address is forwarded to Facebook by GET requests, which are triggered by Facebook code snippets. The IP address enables Facebook to keep track of the website page visits associated with that address.

75.

Facebook also places cookies on visitors' computers. It then uses these cookies to store information about each user. For example, the "c_user" cookie is a unique identifier that identifies a Facebook user's ID. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user has one—and only one—unique c_user cookie. Facebook uses the c_user cookie to record user activities and communications.

76.

The data supplied by the c_user cookie allows Facebook to identify the Facebook account associated with the cookie. One simply needs to log into Facebook, and then type www.facebook.com/#, with the c_user identifier in place of the "#." For example, the c_user cookie for Mark Zuckerberg is 4. Logging into Facebook and typing www.facebook.com/4 in the web browser retrieves Mark Zuckerberg's Facebook page: www.facebook.com/zuck.

77.

Similarly, the "lu" cookie identifies the last Facebook user who logged in using a specific browser. Like IP addresses, cookies are included with each request that a user's browser makes to Facebook's servers. Facebook employs similar cookies such as "datr," "fr," "act," "presence," "spin," "wd," "xs," and "fbp" cookies to track users on websites across the internet.[48] These cookies allow Facebook to easily link the browsing activity of its users to their real-world identities, and such highly sensitive data as medical information, religion, and political preferences.[49]

---

[48] *See, e.g.*, https://techexpertise.medium.com/facebook-cookies-analysis-e1cf6ffbdf8a#:~:text=browser%20session%20ends.%E2%80%9Cdatr%E2%80%9D,security%20and%20site%20integrity%20features.

[49] *See, e.g.*, https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_plugins.pdf

78.

Facebook also uses browser fingerprinting to uniquely identify individuals. Web browsers have several attributes that vary between users, like the browser software system, plugins that have been installed, fonts that are available on the system, the size of the screen, color depth, and more. Together, these attributes create a fingerprint that is highly distinctive. The likelihood that two browsers have the same fingerprint is at least as low as 1 in 286,777, and the accuracy of the fingerprint increases when combined with cookies and the user's IP address. Facebook recognizes a visitor's browser fingerprint each time a Facebook button is loaded on a third-party website page. Using these various methods, Facebook can identify individual users, watch as they browse third-party websites like www.wkhs.com, and target users with advertising based on their web activity.

F. Defendant has discretely embedded the Meta Pixel tool on its website, resulting in the capture and disclosure of customers' protected health information to Facebook.

79.

A third-party website that incorporates Meta Pixel benefits from the ability to analyze a user's experience and activity on the website to assess the website's functionality and traffic. The third-party website also gains information from its customers through Meta Pixel that can be used to target them with advertisements, as well as to measure the results of advertisement efforts.

80.

Facebook's intrusion into the personal data of the visitors to third-party websites incorporating the Meta Pixel is both significant and unprecedented. When Meta Pixel is incorporated into a third-party website, unbeknownst to users and without their consent, Facebook gains the ability to surreptitiously gather every user interaction with the website ranging from what the user clicks on to the personal information entered on a website search bar. Facebook aggregates this data against all websites.[50] Facebook benefits from obtaining this information because it improves its advertising network, including its machine-learning algorithms and its ability to identify and target users with ads.

81.

Facebook provides websites using Meta Pixel with the data it captures in the "Meta Pixel page" in Events Manager, as well as tools and analytics to reach these individuals through future Facebook ads.[51] For example, websites can use this data to create "custom audiences" to target the

[50] *See, e.g.*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142

[51] *See, e.g.*, https://www.facebook.com/business/help/742478679120153?id=1205376682832142

specific Facebook user, as well as other Facebook users who match "custom audience's" criteria.[52] Businesses that use Meta Pixel can also search through Meta Pixel data to find specific types of users to target, such as men over a certain age.

82.

Meta Pixel is wildly popular and embedded on millions of websites, including many websites that are used to store and convey sensitive medical information. Businesses install the Meta Pixel software code to help drive and decode key performance metrics from visitor traffic to their websites.[53] Businesses also use the Meta Pixel to build custom audiences on Facebook that can be used for their own advertising purposes.[54]

83.

Shockingly, Meta Pixel is incorporated on many websites that are used to store and convey sensitive medical information, that by law must be kept private. Recently, investigative journalists have determined that Meta Pixel is embedded on the websites of many of the top hospitals in the United States and on the password-protected patient portals of many healthcare systems.[55] This results in sensitive medical information being collected and then sent to Facebook when a user interacts with these hospital websites. For example, when a user on many of these hospital websites clicks on a "Schedule Online" button next to a doctor's name, Meta Pixel sends the text of the button, the doctor's name, and the search term (such as "cardiology") used to find the doctor to Facebook. If the hospital's website has a drop-down menu to select a medical condition in connection with locating a doctor or making an appointment, that condition is also transmitted to Facebook through Meta Pixel.

84.

Facebook has designed the Meta Pixel such that Facebook receives information about patient activities on hospital websites as they occur in real time. Indeed, the moment that a patient takes any action on a webpage that includes the Meta Pixel—such as clicking a button to register, login, or logout of a patient portal or to create an appointment—Facebook code embedded on that

---

[52] *See, e.g.*, https://developers.facebook.com/docs/marketing-api/reference/custom-audience/

[53] https://instapage.com/blog/meta-pixel

[54] https://instapage.com/blog/meta-pixel

[55] *See, e.g.*, https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

page redirects the content of the patient's communications to Facebook while the exchange of information between the patient and hospital is still occurring.

85.

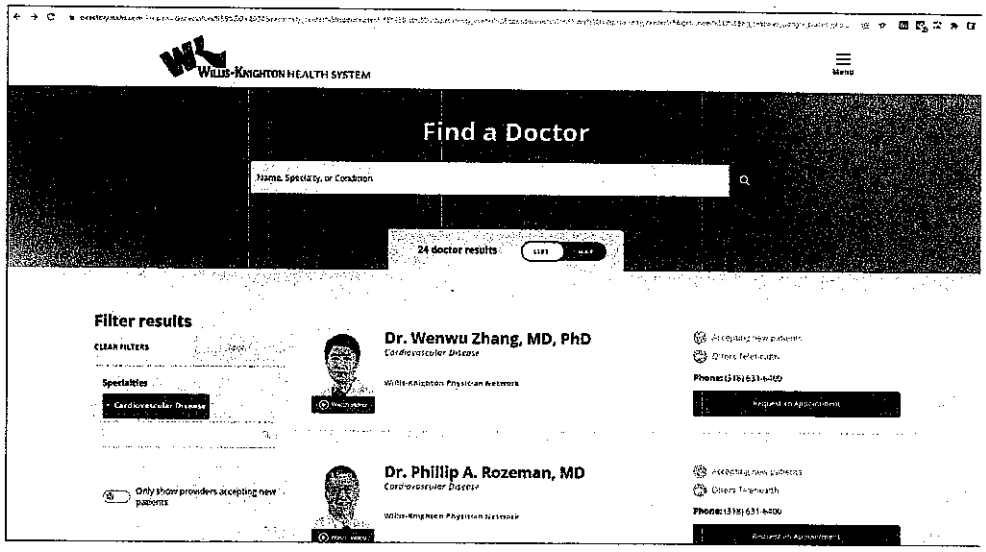
Defendant is among the hospital systems who have embedded Meta Pixel on their websites. When a patient enters their personal information through Defendant's websites that incorporate Meta Pixel, such as to locate a doctor or make an appointment, this information, including what the patient is being treated for, is transmitted to Facebook *via* the Meta Pixel. The acquisition and disclosure of these communications occurs contemporaneously with the transmission of these communications by patients.

86.

This data, which can include health conditions (*e.g.*, addiction, Alzheimer's, heart disease), diagnoses, procedures, test results, the treating physician, medications, and other personally identifying information ("Personal Health Information"), is obtained and used by Facebook, as well as other parties, for the purpose of targeted advertising. Worse, by correlating users' Facebook profiles—profiles that include such details as a user's employment history and age—Facebook gains an intimate personal profile of patients without patients' consent. Indeed, these tracking practices allow Facebook to gain an unprecedented degree of personalized information, including an individual's health history, likes, dislikes, interests, and habits over a significant amount of time, without affording users meaningful opportunity to control or prevent the unauthorized exploration of their private lives.

87.

For example, a patient searching for a doctor on Defendant's website is asked to provide a variety of information to filter the various physicians available to treat various medical conditions, including the doctor's specialty, the patient's condition, the patient's address, the patient's language preference, and other information that the patient provides.

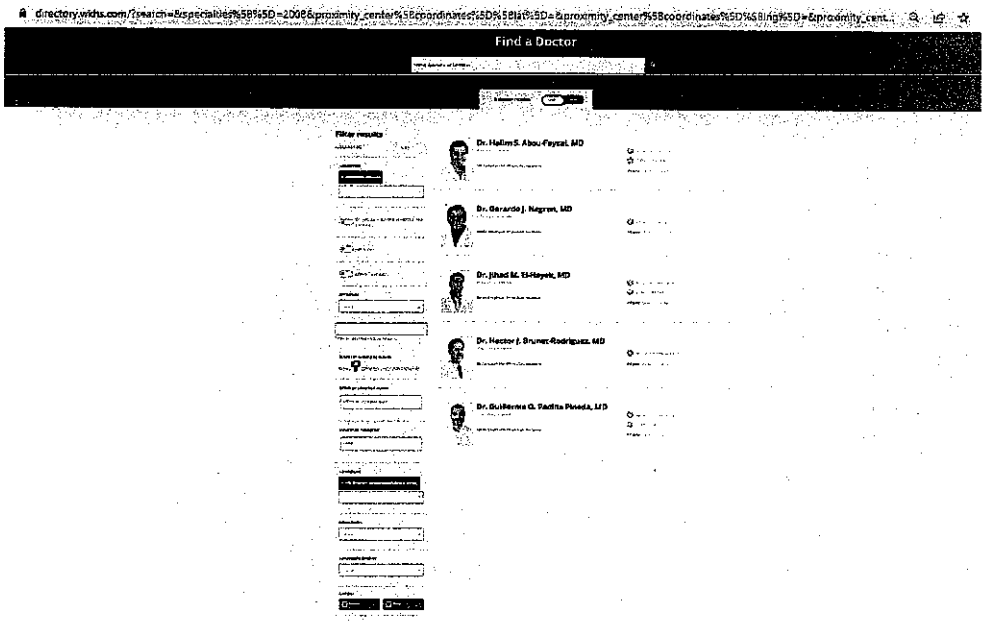


88.

All this data is disclosed to Facebook in real time as patients transmit their information, along with other data, such as patient's unique Facebook ID that is captured by the c_user cookie, which allows Facebook to link this information to patients' unique Facebook accounts. Defendant also discloses other personally identifying information to Facebook, such as patient IP addresses, cookie identifiers, browser-fingerprints, and device identifiers.

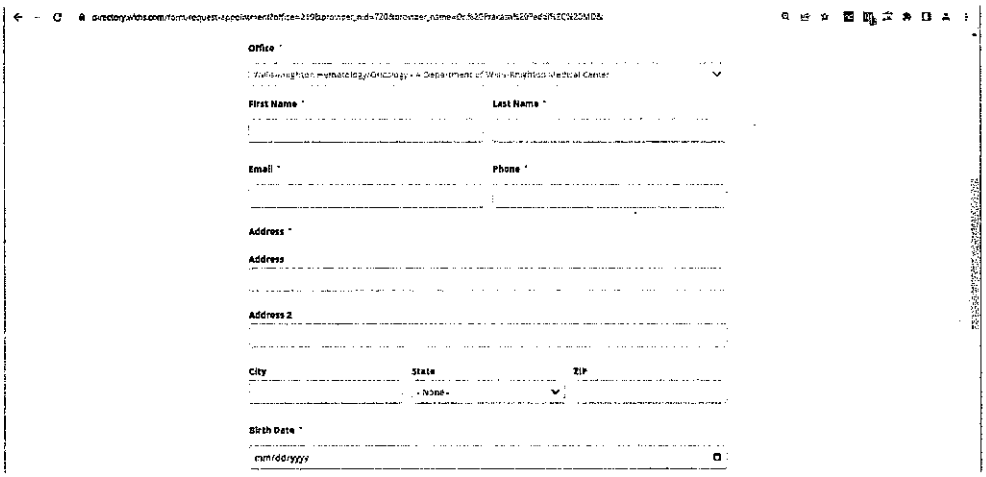
89.

Defendant discloses such personally identifying information and sensitive medical information even when patients are searching for doctors to assist with them conditions such as substance abuse and addiction.



90.

Likewise, a patient who desires an appointment with a specific doctor is asked to fill out an extensive online questionnaire, which includes information such as the doctor's name, the reason for the visit, to fill out also requests the patient's name, date of birth, address, and contact information. All this information is acquired by Defendant and forwarded to Facebook via the Meta Pixel contemporaneously with its transmission by patients.



91.

Defendant also discloses patient information from other sections of its website including (but not limited to) communications that are captured by the website's search bar, communications that are captured when a patient searches for "Services" offered by Defendant, communications made by patients using the website's Bill Pay/Financials function, and communications made when patients are researching specific medical conditions such as COVID-19. Defendant also makes similar disclosures to Facebook, Google, and other parties when click on the "Log in" buttons of the password protected portions of its website, including its patient portal and bill pay functions, confirming to these companies that the website users are Willis-Knighton patients.

92.

As the above demonstrates, knowing what information a patient is reviewing on Defendant's website can reveal deeply personal and private information. For example, a simple search for "pregnancy" on Defendant's website tells Facebook that the patient is likely pregnant. Indeed, Facebook might know that the patient is pregnant before the patient's close family and friends. Likewise, most patients would not want it made public that they were seeking treatment

for substance abuse. But there is nothing visible on Defendant's website that would indicate to patients that, when they use Defendant's search function, their personally identifiable data and the precise content of their communications with Defendant are being automatically captured and made available to Facebook, who can then use that information for advertising purposes even when patients search for treatment options for sensitive medical conditions such as cancer or substance abuse.

93.

The amount of data collected is significant. Via the Meta Pixel, when patients interact with its website, Defendant discloses a full-string, detailed URL to Facebook, which contains the name of the website, folder and sub-folders on the webserver, and the name of the precise file requested. For example, when a patient types a search term into the search bar on Defendant's website, the website returns links to information relevant to the search term. When patients then click these links, a communication is created that contains a GET request and a full-string detailed URL.

94.

Facebook's Meta Pixel collects and forwards this data to Facebook, including the full referral URL (including the exact subpage of the precise terms being reviewed) and Facebook then correlates the URL with the patient's Facebook user ID, time stamp, browser settings, and even the type of browser used. In short, the URLs, by virtue of including the particular document within a website that a patient views, reveal a significant amount of personal data about a patient. The captured search terms and the resulting URLs divulge a patient's medical issues, personal interests, queries, and interests on third-party websites operating outside of Facebook's platform.

95.

The transmitted URLs contain both the "path" and the "query string" arising from patients' interactions with Defendant's websites. The path identifies where a file can be found on a website. Likewise, a query string provides a list of parameters. The query string parameters in a search, for example, can indicate that a search was done at Defendant's website for information about a particular condition such as HIV. In other words, the Meta Pixel captures information that connects a particular user to a particular healthcare provider.

96.

Defendant also provides Facebook with details about online forms that patients fill out in the form of POST requests, such as when a patient utilizes the Willis-Knighton website's "Find A

Doctor" function. All the information that patients provide when filling out these forms are also disclosed to Facebook.

97.

The contents of patients' search terms shared with Facebook plainly relate to (and disclose) the past, present, or future physical or mental health or condition of individual patients who interact with Defendant's website. Worse, no matter how sensitive the area of the Defendant's website that a patient reviews, the referral URL is acquired by Facebook along with cookies that precisely identify the patient.

98.

The nature of the collected data is also important. Defendant's unauthorized disclosures result in Facebook obtaining a comprehensive browsing history of an individual patient, no matter how sensitive the patient's medical condition. Facebook is then able to correlate that history with the time of day and other user actions on Defendant's website. This process results in Facebook acquiring a vast repository of personal data about patients—all without their knowledge or consent.

99.

By compelling visitors to its websites to disclose personally identifying data and sensitive medical information to Facebook and other third parties, Defendant knowingly discloses information that allows Facebook and other advertisers to link its patients Personal Health Information to their private identities and target them with advertising. Defendant intentionally shared the Personal Health Information of its patients with Facebook in order to gain access to the benefits of the Meta Pixel tool.

100.

Defendant facilitated the disclosure of Plaintiff's Personal Health information, including sensitive medical information, to Facebook (and/or other third parties), without her consent or authorization, when she entered information on the website that Defendant maintains at www.wkhs.com. Plaintiff continued to have her privacy violated when Defendant permitted Facebook and other companies to send her targeted advertising related to her medical condition.

101.

For example, Plaintiff is an individual with a Facebook account who visited Defendant's website in 2022 at www.wkhs.com and entered data, including sensitive medical information, such

as details about her medical condition and doctor. The information that Plaintiff transmitted included queries about a medical procedure of a sensitive nature.

102.

After entering her medical information on Defendant's website, Plaintiff began receiving ads on her Facebook page related to her medical condition.

103.

As a result of Defendant's compliance and aid in the illegal interception and disclosure of her Personal Health Information, Plaintiff received advertisements that were specifically tailored to her Personal Health Information, including sensitive medical information, that she entered on Defendant's website. These advertisements were tailored and directed to Plaintiff by Facebook as part of Facebook's advertising business in which Facebook profits from providing third parties with access to those individuals most likely to be interested in their products or services, otherwise known as the "target audience."[56]

104.

Defendant knew that by embedding Meta Pixel – a Facebook advertising tool – it was permitting Facebook to collect, use, and share Plaintiff's and the Class Members' Personal Health Information, including sensitive medical information and personally identifying data. Defendant was also aware that such information would be shared with Facebook simultaneously with patients' interactions with its websites. Defendant made the decision to barter its patients' Personal Health Care Information to Facebook because it wanted access to the Meta Pixel tool. While that bargain may have benefited Defendant and Facebook, it also betrayed the privacy rights of Plaintiff and Class Members.

G. Plaintiff and the Class Members did not consent to the interception and disclosure of their protected health information.

105.

Plaintiff and Class Members had no idea when they interacted with Defendant's websites that their personal data, including sensitive medical data, was being collected and transmitted to Facebook. That is because, among other things, Meta Pixel is seamlessly integrated into Defendant's websites and is invisible to patients visiting those websites.

[56] *See, e.g.*, https://www.facebook.com/business/ads/ad-targeting?content

106.

For example, when Plaintiff visited Defendant's website in 2022 at www.wkhs.com, there was no indication that Meta Pixel was embedded on that website or that it would collect and transmit her sensitive medical data to Facebook.

107.

Plaintiff and her fellow Class Members could not consent to Defendant's conduct when there was no indication that their sensitive medical information would be collected and transmitted to Facebook in the first place.

108.

While Defendant purports to have a "Web Privacy Policy" and "Privacy Practices," those policies and practices are effectively hidden from patients, buried inside hyperlinks concealed in at the bottom of Defendant's homepage in type so small as to be unreadable to many visitors:

109.

While disclosing that its website contains "cookies", Defendant's "Web Privacy Policy" falsely promises patients that the "cookies … are not used to identify individuals."[57] Contrary to that representation, Defendant's website automatically transmits personally identifiable information to Facebook using multiple cookies, including c_user, datra, fr, and xs cookies. Defendant's "Web Privacy Policy" or "Notice of Privacy Practices" give no indication to patients

[57] *See, e.g.*, https://www.wkhs.com/Website-Info/Web-Privacy-Policy

that Defendant routinely allows Facebook to capture and exploit patients' Personal Health Information. Indeed, Defendant expressly promises in its "Privacy Practices" that "We will not use and disclose your Protected Health Information for marketing purposes without your written consent."[58]

110.

Even if a patient stumbled upon Defendant's carefully hidden "Web Privacy Policy" and "Notice of Privacy Practices," nothing in that notice would be understood by any reasonable patient to mean that Defendant is routinely allowing Facebook to capture and exploit patients' Personal Health Information.

111.

Defendant does not have a legal right to share Plaintiff's and Class Members' Protected Health Information without their written consent because this information is protected from such disclosure by law.[59] Much less is Defendant permitted to disclose patients' protected health information to advertising and marketing companies like Facebook without express written authorization from patients.[60] Defendant failed to obtain a valid written authorization from Plaintiffs or any of the Class Members to allow the capture and exploitation of their personally identifiable information and the contents of their communications for marketing purposes.

112.

A patient's reasonable expectation that their health care provider will not share their information with third parties for marketing purposes is not subject to waiver via an inconspicuous privacy policy hidden away on a company's website. Such "Browser-Wrap" statements do not create an enforceable contract against consumers. Further, Defendant expressly promised its patients that it would never sell or use their Personal Health Information for marketing purposes without express authorization.

113.

Accordingly, Defendant lacked authorization to intercept, collect, and disclose Plaintiffs and Class Members' Personal Health Information to Facebook or aid in the same.

---

[58] *See, e.g.*, https://www.wkhs.com/about/notice-of-privacy-practices

[59] *See, e.g.*, La. R.S. 51:3074; (*see also, e.g.*, 45 C.F.R. §164.508).

[60] *See, e.g.*, 48 La. Admin. Code Pt 1, §9319.

H. Defendant's disclosures of Plaintiff and the Class Members' Personal Health Information to Facebook are unnecessary.

114.

There is no information anywhere on the websites operated by Defendant that would alert patients that their most private information (such as their identifiers, their medical conditions, and their medical providers) is being automatically transmitted to Facebook. Nor are the disclosures of patient Personal Health Information to Facebook necessary for Defendant to maintain its healthcare website.

115.

For example, it possible for a health care website to provide a doctor search function without allowing disclosures to third-party advertising companies about patient sign ups or appointments. It is also possible for a website developer to utilize tracking tools without allowing disclosure of patients' Personal Healthcare Information to companies like Facebook. Likewise, it is possible for Defendant to provide medical services to patients without sharing their Personal Health Information with Facebook so that this information can be exploited for advertising purposes.

116.

Despite these possibilities, Defendant willfully chose to implement Meta Pixel on its websites and aid in the disclosure of personally identifiable information and sensitive medical information about its patients, as well as the contents of their communications with Defendant, to third-parties, including Facebook.

I. Plaintiffs and Class Members have a reasonable expectation of privacy in their Personal Health Information, especially with respect to sensitive medical information.

117.

Plaintiffs and Class Members have a reasonable expectation of privacy in their Personal Health Information, including personally identifying data and sensitive medical information. Defendant's surreptitious interception, collection, and disclosure of patients' Personal Health Information to Facebook violated Plaintiffs and Class Member's privacy interests.

118.

Patient Personal Health Information is specifically protected by law. *See, e.g.,* La. R.S. 51:3074, *and,* 48 La. Admin. Code Pt 1, §9319. The prohibitions against disclosing personally identifying information include prohibitions against disclosing personally identifying data such

patient names, IP addresses, and other unique characteristics or codes. *See, e.g.*, La. Admin. Code Pt 1, §505; (*see also, e.g.*, 45 C.F.R. §164.514). This legal framework applies to health care providers, such as Defendant.

119.

Given the public policy expressed by these laws, Plaintiff and Class Members had a reasonable expectation of privacy in their protected health information.

120.

Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the disclosure of sensitive medical information violates expectations of privacy that have been established as general social norms.

121.

Privacy polls and studies also uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

122.

For example, a recent study by Consumer Reports showed that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believed that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[61]

123.

Users act consistently with these preferences. For example, following a new rollout of the iPhone operating software – which asks users for clear, affirmative consent before allowing companies to track users – 85 percent of worldwide users and 94 percent of U.S. users chose not to share data when prompted.[62]

124.

The concern about sharing personal medical information is compounded by the reality that advertisers view this type of information as particularly valuable. Indeed, having access to the

[61] *See, e.g.*, https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/

[62] *See, e.g.*, https://www.wired.co.uk/article/apple-ios14-facebook

data women share with their healthcare providers allows advertisers to obtain data on children before they are even born. As one recent article noted, "What is particularly worrying about this process of datafication of children is that companies like [Facebook] are harnessing and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[63]

125.

Many privacy law experts have expressed serious concerns about patients' sensitive medical information being disclosed to third-party companies like Facebook. As those critics have pointed out, having a patient's personal health information disseminated in ways the patient is unaware of could have serious repercussions, including affecting their ability to obtain life insurance, how much they might pay for such coverage, the rates they might be charged on loans, and the likelihood of their being discriminated against.

J. Plaintiffs' Personal Health Data that Defendant collected, disclosed, and used is Plaintiffs' property, has economic value, and its illicit disclosure has caused Plaintiffs harm.

126.

It is common knowledge that there is an economic market for consumers' personal data – including the kind of data that Defendant has collected and disclosed from Plaintiffs and Class Members.

127.

In 2013, the *Financial Times* reported that the data-broker industry profits from the trade of thousands of details about individuals, and that within that context, "age, gender and location information" were being sold for approximately "$0.50 per 1,000 people."[64]

128.

In 2015, *TechCrunch* reported that "to obtain a list containing the names of individuals suffering from a particular disease," a market participant would have to spend about "$0.30" per name.[65] That same article noted that "Data has become a strategic asset that allows companies to

[63] https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/

[64] *See, e.g.*, https://ig.ft.com/how-much-is-your-personal-data-worth/

[65] *See, e.g.*, https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

acquire or maintain a competitive edge" and that the value of a single user's data can vary from $15 to more than $40 per user.[66]

129.

In a 2021 Washington Post article, the legal scholar Dina Srinivasan said that consumers "should think of Facebook's cost as [their] data and scrutinize the power it has to set its own price."[67] This price is only increasing. According to Facebook's own financial statements, the value of the average American's data in advertising sales rose from $19 to $164 per year between 2013 and 2020.[68]

130.

Despite the protections afforded by law, there is an active market for health information. Medical information obtained from health providers garners substantial value because of the fact that it is not generally available to third party data marketing companies because of the strict restrictions on disclosure of such information by state laws and provider standards, including the Hippocratic oath. Even with these restrictions, however, a multi-billion-dollar market exists for the sale and purchase of such private medical information.[69]

131.

Further, individuals can sell or monetize their own data if they so choose. For example, Facebook has offered to pay individuals for their voice recordings,[70] and has paid teenagers and adults up to $20 a month plus referral fees to install an app that allows Facebook to collect data on how individuals use their smart phones.[71]

132.

A myriad of other companies and apps such as DataCoup, Nielsen Computer, Killi, and UpVoice also offer consumers money in exchange for access to their personal data.[72]

---

[66] *See, e.g.*, https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/

[67] *See, e.g.*, https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

[68] *See, e.g.*, https://www.washingtonpost.com/technology/2021/08/29/facebook-privacy-monopoly/

[69] *See, e.g.*, https://revealnews.org/blog/your-medical-data-is-for-sale-and-theres-nothing-you-can-do-about-it/; *see also https://slate.com/technology/2022/06/health-data-brokers-privacy.html*

[70] *See, e.g.*, https://www.theverge.com/2020/2/20/21145584/facebook-pay-record-voice-speech-recognition-viewpoints-proununciations-app

[71] *See, e.g.*, https://www.cnbc.com/2019/01/29/facebook-paying-users-to-install-app-to-collect-data-techcrunch.html

[72] *See, e.g.*, https://www.creditdonkey.com/best-apps-data-collection.html; *see also* https://www.monetha.io/blog/rewards/earn-money-from-your-data/

133.

Given the monetary value that data companies like Facebook have already paid for personal information in the past, Defendant has deprived Plaintiff and the Class Members of the economic value of their sensitive medical information by collecting, using, and disclosing that information to Facebook and other third parties without consideration for Plaintiff's and the Class Members' property.

K. Defendant is enriched by making unlawful, unauthorized, and unnecessary disclosures of its customers' protected health information.

134.

In exchange for disclosing Personal Health Information about its patients, Defendant is compensated by Facebook with enhanced online advertising services, including (but not limited to) re-targeting and enhanced analytics functions.

135.

Re-targeting is a form of online targeted advertising that targets users with ads based on their previous internet actions, which is facilitated through the use of cookies and tracking pixels. Once an individual's data is disclosed and shared with a third-party marketing company, the advertiser is able to show ads to the user elsewhere on the internet.

136.

For example, retargeting could allow a web-developer to show advertisements on other websites to customers or potential customers based on the specific communications exchanged by a patient or their activities on a website. Using the Meta Pixel, a website could target ads on Facebook itself or on the Facebook advertising network. The same or similar advertising can be accomplished via disclosures to other third-party advertisers and marketers.

137.

Once personally identifiable information relating to patient communications is disclosed to third parties like Facebook, Defendant loses the ability to control how that information is subsequently disseminated and exploited.

138.

The monetization of the data being disclosed by Defendant, both by Defendant and Facebook, demonstrates the inherent value of the information being collected.

L. Facebook's history of egregious privacy violations.

139.

Defendant knew or should have known that Facebook could not be trusted with its patients' sensitive medical information.

140.

Due to its ability to target individuals based on granular data, Facebook's ad-targeting capabilities have frequently come under scrutiny. For example, in June 2022, Facebook entered into a settlement with the Department of Justice regarding its Lookalike Ad service, which permitted targeted advertising by landlords based on race and other demographics in a discriminatory manner. That settlement, however, reflected only the latest in a long history of egregious privacy violations by Facebook.

141.

In 2007, when Facebook launched "Facebook Beacon," users were unaware that their online activity was tracked, and that the privacy settings originally did not allow users to opt-out. As a result of widespread criticism, Facebook Beacon was eventually shut down.

142.

Two years later, Facebook made modifications to its Terms of Service, which allowed Facebook to use anything a user uploaded to its site for any purpose, at any time, even after the user ceased using Facebook. The Terms of Service also failed to provide for any way for users to completely delete their accounts. Under immense public pressure, Facebook eventually returned to its prior Terms of Service.

143.

In 2011, Facebook settled charges with the Federal Trade Commission relating to its sharing of Facebook user information with advertisers, as well as its false claim that third-party apps were able to access only the data they needed to operate when, in fact, the apps could access nearly all of a Facebook user's personal data. The resulting Consent Order prohibited Facebook from misrepresenting the extent to which consumers can control the privacy of their information, the steps that consumers must take to implement such controls, and the extent to which Facebook makes user information available to third parties.[73]

[73] https://www.ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter

144.

Facebook found itself in another privacy scandal in 2015 when it was revealed that Facebook could not keep track of how many developers were using previously downloaded Facebook user data. That same year, it was also revealed that Facebook had violated users' privacy rights by harvesting and storing Illinois' users' facial data from photos without asking for their consent or providing notice. Facebook ultimately settled claims related to this unlawful act for $650 million.

145.

In 2018, Facebook was again in the spotlight for failing to protect users' privacy. Facebook representatives testified before Congress that a company called Cambridge Analytics may have harvested the data of up to 87 million users in connection with the 2016 election. This led to another FTC investigation in 2019 into Facebook's data collection and privacy practices, resulting in a record-breaking five-billion-dollar settlement.

146.

Likewise, a different 2018 report revealed that Facebook had violated users' privacy by granting access to user information to over 150 companies.[74] Some companies were even able to read users' private messages.

147.

In June 2020, after promising users that app developers would not have access to data if users were not active in the prior 90 days, Facebook revealed that it still enabled third-party developers to access this data.[75] This failure to protect users' data enabled thousands of developers to see data on inactive users' accounts if those users were Facebook friends with someone who was an active user.

148.

On February 18, 2021, the New York State Department of Financial Services released a report detailing the significant privacy concerns associated with Facebook's data collection practices, including the collection of health data. The report noted that while Facebook maintained a policy that instructed developers not to transmit sensitive medical information, Facebook received, stored, and analyzed this information anyway. The report concluded that "[t]he

[74] https://www.cnbc.com/2018/12/19/facebook-gave-amazon-microsoft-netflix-special-access-to-data-nyt.html

[75] https://fortune.com/2020/07/01/facebook-user-data-apps-blunder/

information provided by Facebook has made it clear that Facebook's internal controls on this issue have been very limited and were not effective … at preventing the receipt of sensitive data."[76]

149.

The New York State Department of Financial Service's concern about Facebook's cavalier treatment of private medical data is not misplaced. In June 2022, the FTC finalized a different settlement involving Facebook's monetizing of sensitive medical data. In that case, the more than 100 million users of Flo, a period and ovulation tracking app, learned something startling: the company was sharing their data with Facebook.[77] When a user was having her period or informed the app of her intention to get pregnant, Flo would tell Facebook, which could then use the data for all kinds of activities including targeted advertising. In 2021, Flo settled with the Federal Trade Commission for lying to its users about secretly sharing their data with Facebook, as well as with a host of other internet advertisers, including Google, Fabric, AppsFlyer, and Flurry. The FTC reported that Flo "took no action to limit what these companies could do with users' information."[78]

150.

Facebook employees have admitted that the company has lax protections for sensitive user data. Facebook engineers on the ad business product team conceded in a 2021 privacy review that "We do not have an adequate level of control and explainability over how our systems use data, and thus we can't confidently make controlled policy changes or external commitments such as 'we will not use X data for Y purpose."[79]

151.

These revelations were confirmed by an article published by the Markup in 2022, which found during the course of its investigation that Facebook's purported "filtering" failed to discard even the most obvious forms of sexual health information. Worse, the article found that the data that the Meta Pixel was sending Facebook from hospital websites not only included details such as patients' medications, descriptions of their allergic reactions, details about their upcoming doctor's appointments, but also included patients' names, addresses, email addresses, and phone numbers.[80]

---

[76] https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

[77] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

[78] https://slate.com/technology/2022/06/health-data-brokers-privacy.html

[79] https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes

[80] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites

152.

Despite knowing that the Meta Pixel code embedded in its websites was sending patients' Personal Health Information to Facebook, Defendant did nothing to protect its patients from egregious intrusions into its patients' privacy, choosing instead to benefit at those patients' expense.

M. Numerous hospital systems have acknowledged the harmful disclosures of patient health information to Facebook via the Meta Pixel on their websites.

153.

After publication of the Markup's investigative article in June 2022, hospital systems around the United States began self-reporting data breaches arising from their installation of pixel technology on their websites.[81]

154.

For example, in August 2022, Novant Health informed approximately 1.3 million patients that their medical data was disclosed to Facebook due to the installation of the Facebook Meta Pixel on the hospital system's websites.[82] Novant Health's data breach announcement conceded that the Meta Pixel tool installed on its websites "allowed certain private information to be transmitted to Meta from the Novant Health website."[83] Novant Health further admitted that the information about its patients that was disclosed to Facebook included "an impacted patient's: demographic information such as email address, phone number, computer IP address, and contact information entered into Emergency Contacts or Advanced Care Planning; and information such as appointment type and date, physician selected, button/menu selections, and/or content typed into free text boxes."[84]

155.

Likewise, in October 2022, Advocate Aurora Health informed approximately 3 million patients that their Personal Health Information had been disclosed to Facebook via the Meta Pixel installed on Advocate Aurora Health's website.[85]

---

[81] https://www.scmagazine.com/analysis/breach/pixel-fallout-expands-community-health-informs-1-5m-of-unauthorized-disclosure

[82] https://www.scmagazine.com/analysis/breach/1-3m-novant-health-patients-notified-of-unintended-disclosure-via-facebook-pixel

[83] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[84] https://www.novanthealth.org/home/about-us/newsroom/press-releases/newsid33987/2672/novant-health-notifies-patients-of-potential-data-privacy-incident-.aspx

[85] https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3

156.

Advocate Aurora Health's data breach notification conceded that patient information had been transmitted to third parties including Facebook and Google when patients used the hospital system's website.[86]

157.

Advocate Aurora Health further admitted that a substantial amount of its patients' Personal Health Information has been shared with Facebook and Google including patients' "IP address; dates, times, and/or locations of scheduled appointments; your proximity to an Advocate Aurora Health location; information about your provider; [and] type of appointment or procedure."[87] Even more troubling, Advocate Aurora Health admitted that "[w]e cannot confirm how vendors used the data they collected."[88]

158.

Advocate Aurora Health claimed that, in conjunction with its data breach notice, the hospital system had "disabled and/or removed the pixels from our platforms and launched an internal investigation to better understand what patient information was transmitted to our vendors."[89] Advocate Aurora Health also promised its 3 million patients that the company had instituted an "enhanced, robust technology vetting process" to prevent such disclosures of its patients' Personal Health Information in the future.[90]

159.

Similarly, in October 2022, WakeMed notified more than 495,000 patients that their Personal Health Information had been transmitted to Facebook through the use of tracking pixels installed on its websites.[91] In announcing this data breach, WakeMed admitted that the Facebook Meta Pixel tool had been installed on its website resulting in the transmission of patient information to Facebook.[92] WakeMed further admitted that "[d]epending on the user's activity, the data that may have been transmitted to Facebook could have included information such as: email address, phone number, and other contact information; computer IP address; emergency contact information; information provided during online check-in, such as allergy or medication

[86] https://www.advocateaurorahealth.org/
[87] https://www.advocateaurorahealth.org/pixel-notification/faq
[88] https://www.advocateaurorahealth.org/pixel-notification/faq
[89] https://www.advocateaurorahealth.org/pixel-notification/faq
[90] https://www.advocateaurorahealth.org/pixel-notification/faq
[91] https://healthitsecurity.com/news/wakemed-faces-data-breach-lawsuit-over-meta-pixel-use
[92] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident

information; COVID vaccine status; and information about an upcoming appointment, such as appointment type and date, physician selected, and button/menu selections."[93]

160.

WakeMed also conceded that it had no idea what Facebook had done with the Personal Health Information that WakeMed had disclosed about its patients.[94] Like other the other hospital systems who have come clean about their use of the Meta Pixel tool, WakeMed promised its patients that it had "proactively disabled Facebook's pixel" and had "no plans to use it in the future without confirmation that the pixel no longer has the capacity to transmit potentially sensitive or identifiable information."[95]

161.

In November 2022, the fallout from hospital systems' use of the Meta Pixel tool expanded when Community Health Network informed 1.5 million of its patients that their personal health information had been routinely transmitted and disclosed to Facebook since at least April 2017.[96]

162.

In its data breach notice, Community Health admitted that it had "discovered through our investigation that the configuration of certain technologies allowed for a broader scope of information to be collected and transmitted to each corresponding third-party tracking technology vendor (e.g., Facebook and Google) than Community had ever intended." Community Health further conceded that its use of the Meta Pixel and related third-party tracking technologies had resulted in surreptitiously recording and transmitting a wide range of patient engagements with its websites, including "includes scheduling an appointment online or directly with a provider" and "seeking treatment at a Community or affiliated provider location."[97]

163.

Community Health, like WakeMed, Novant, and Advocate Aurora Health, also promised its patients that it had disabled or removed the third-party tracking technologies that it had installed on its website and had instituted new "evaluation and management processes for all website

---

[93] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident
[94] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident
[95] https://www.wakemed.org/about-us/news-and-media/wakemed-news-releases/wakemed-notifies-patients-of-potential-data-privacy-incident
[96] https://healthitsecurity.com/news/community-health-network-notifies-1.5m-of-data-breach-stemming-from-tracking-tech; *see also* https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach
[97] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

technologies moving forward."[98] Community Health, however, also conceded that it had no idea how Facebook or other third parties had exploited the patient Personal Health Information that had been disclosed to them via the pixel technology.

164.

As these data breach announcements demonstrate, there is widespread knowledge within the health care community that installation of the Meta Pixel tool on hospital websites results in the disclosure of patients' Personal Health Information Facebook. There is also widespread recognition that such disclosures are not only illegal but fundamentally unethical, given the privacy rights involved.

CONTRA NON VALENTUM
(AND/OR THE CONTINUING TORT DOCTRINE)

165.

The applicable prescriptive period has been suspended as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

166.

Defendant seamlessly incorporated Meta Pixel and other trackers into its websites, providing no indication to users that they were interacting with a website enabled by Meta Pixel. Defendant had knowledge that its websites incorporated Meta Pixel and other trackers yet failed to disclose that by interacting with Meta-Pixel enabled websites that Plaintiffs and Class Members' sensitive medical information would be intercepted, collected, used by, and disclosed to Facebook.

167.

Plaintiff and Class Members could not with due diligence have discovered the full scope of Defendants' conduct, because there were no disclosures or other indication that they were interacting with websites employing Meta Pixel.

168.

The earliest that Plaintiff and Class Members, acting with due diligence, could have reasonably discovered this conduct would have been on June 15, 2022, following the release of the Markup's investigation.

[98] https://www.ecommunity.com/notice-third-party-tracking-technology-data-breach

169.

All applicable prescriptive periods have also been suspended by operation of the discovery rule and/or the continuing tort doctrine. Defendant's illegal interception and disclosure of patients' Personal Health Information has continued unabated through the date of the filing of this Petition. What's more, Defendant was under a duty to disclose the nature and significance of their data collection practices but did not do so. Defendant is therefore estopped from relying on any prescription defenses.

CLASS ACTION ALLEGATIONS

170.

Plaintiff brings this action pursuant to Articles 591(B)(2) and/or (B)(3) of the Louisiana Code of Civil Procedure on behalf of herself and a class of others similarly situated, preliminarily defined as follows: "All current citizens of the state of Louisiana who, from June 15, 2012 thru [the Date of Certification] are, or were, actual or prospective patients of Defendant or any of its affiliates and who exchanged communications on one or more of Defendant's websites."[99]

171.

Excluded from the proposed Class are (1) any Judge or Magistrate presiding over this action and members of their families; (2) the Defendant, Defendant's subsidiaries, affiliates, parents, successors, predecessors, and any entity in which the Defendant or its parent has a controlling interest and their current or former employees, officers, and directors; and (3) Plaintiff's counsel and Defendant's counsel.

172.

This action is properly maintainable as a class action as provided by Louisiana Code of Civil Procedure Article 591(A) for the reasons described below.

173.

Numerosity: The exact number of class members is unknown at present but is reasonably believed to exceed several thousand persons, such that the joinder of this number of parties as Plaintiffs in one proceeding would be impracticable. The exact number of Class Members can likely be determined by review of information maintained by Defendant.

[99] Plaintiff reserves the right to redefine the Class or and/or add Subclasses, at, or prior to, the class certification stage, in light of any relevant facts or information that might be uncovered in discovery, and/or pursuant to any other direction or instruction from the Court.

174.

Commonality and Predominance: Pursuant to La. C.C.P. Art. 591(A)(2), there exist questions of law and/or fact common to all Class Members, which predominate over any questions affecting only the individual members, including, but not limited to:

a. Whether Defendant's acts and practices violated Plaintiffs and Class Members' privacy rights;

b. Whether Defendant's acts and practices violate La. R.S. 15:1303;

c. Whether Defendant's acts and practices violate La. R.S. 51:3074;

d. Whether Defendant's acts and practices violate 48 La. Admin. Code Pt 1, §9319;

e. Whether Defendant's acts and practices violate La. Admin. Code Pt. 1, §505;

f. Whether Defendant knowingly allowed the surreptitious collection and disclosure of Plaintiffs and Class Members' Personal Health Information to Facebook (and/or other third parties);

g. Whether Defendant profited from disclosures of patient Personal Health Information to third parties including Facebook;

h. Whether Plaintiffs and Class Members are entitled to equitable relief including, but not limited to, injunctive relief, restitution, and/or disgorgement; and

i. Whether Plaintiffs and Class Members are entitled to statutory damages.

175.

Typicality and **Adequacy of Representation:** Plaintiff's claims are typical of the claims of other Class Members and Plaintiff has substantially the same interest in this matter as other Class Members. Plaintiff has retained competent counsel and is committed to the faithful and adequate representation of the Proposed Class. Plaintiff has no interests that are antagonist to, nor in conflict with, the interests of other members of the Class. Plaintiff's claims arise out of the same set of facts and conduct as all other Class Members.

176.

Objectively Defined Class: Pursuant to La. C.C.P. Art. 591(A)(5), the proposed class is defined objectively in terms of ascertainable criteria, such that the Court may determine the constituency of the class for the purposes of the conclusiveness of any judgment that may be rendered. Indeed, the identity of each Class Member can likely be determined by review of information maintained by the Defendant.

177.

Certification is appropriate under Article 591(B)(2), as class-wide injunctive and/or equitable relief is appropriate. In addition, and/or in the alternative, certification is appropriate

under Article 591(B)(3), as the common issues predominate over the individual issues, and the class action is a superior method of adjudicating the controversy.

178.

Plaintiffs anticipate no unusual difficulties in the management of this litigation as a class action. The Class is readily ascertainable and direct notice can likely be provided from the records maintained by Defendant.

179.

For the above reasons, among others, a class action is superior to other available methods for the fair and efficient adjudication of this action. Such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently and without duplication. Separate trials adjudicating the liability of the Defendants will be inefficient and will run the risk of producing inconsistent verdicts. There are no difficulties that would preclude class action treatment of this lawsuit, and no superior alternative exists for the fair and efficient adjudication of this controversy.

CAUSES OF ACTION

COUNT I
Interception and Disclosure of Wire, Electronic, or Oral Communications in Violation of La. R.S. 15:1303
(On Behalf of Plaintiff and the Class)

180.

Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

181.

Plaintiff brings this claim on behalf of herself and all members of the Class.

182.

All conditions precedent to this action have been performed or have occurred.

183.

Louisiana's Electronic Surveillance Act prohibits any person from willfully intercepting, disclosing, or using the contents of any wire or electronic communication that was obtained in violation of the Act. La. R.S. 15:1303. Under the Act, it is unlawful for a person not acting under color of law to intercept a wire, electronic, or oral communication where such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the

constitution or laws of the United States or of the state for the purpose of committing any other injurious act. La. R.S. 15:1303(c)(4).

184.

Any person "whose wire, electronic, or oral communication is intercepted, disclosed, or used in violation of [the Electronic Surveillance Act] shall have a civil cause of action against any person who intercepts, discloses, or uses, or procures for any other person to intercept, disclose, or use such communications." La. R.S. 15:1312.

185.

Defendant qualifies as a person under the statute.

186.

All alleged communications between Plaintiffs or Class Members and Defendant qualify as wire communications under Louisiana law because each communication is made using personal computing devices (*e.g.,* computers, smartphones, tablets) that send and receive communications in whole or in part through the use of facilities used for the transmission of communications aided by wire, cable, or other like connections.

187.

"Intercept" under the Act means the acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device." La. R.S. 15:1302(12).

188.

Defendant engaged in and continues to engage in an "interception" by aiding others (including Facebook) to secretly record the contents of Plaintiff's and Class Members' wire communications. Defendant intercepted Plaintiff's and Class Members' electronic communications for the purpose of committing multiple criminal and tortious acts, including, but not limited to, violating La. R.S. 51:3074 (Protection of Personal Information; Disclosure upon Breach in the Security of Personal Information; Notification Requirements; Exemption), 48 La. Admin. Code Pt 1, § 9319 (Patient Rights and Privacy), La. Admin. Code Pt 1, § 505 (Confidentiality and Disclosure), as well as Louisiana Civil Code Articles 2315, 2316 and/or 2324(A). Defendant also intercepted and disclosed Plaintiff's and Class Members' Personal Health Information for the purpose of committing multiple injurious acts, including depriving

Plaintiff and Class Members of the value of their Personal Health Information by sharing their information without their consent or providing compensation for the same.

189.

The intercepting devices used in this case include, but are not limited to:

a. Plaintiff's and Class Members' personal computing devices;

b. Plaintiff's and Class Members' web browsers;

c. Plaintiff's and Class Members' browser-managed files;

d. Facebook's Meta Pixel;

e. Internet cookies;

f. Defendant's computer servers;

g. Third-party source code utilized by Defendant; and

h. Computer servers of third parties (including Facebook) to which Plaintiff's and Class Members' communications were disclosed.

190.

Under the Act, "contents" are defined to mean "any information concerning the substance, purport, or meaning of that communication." La. R.S. 15:1302(6). Likewise, "Electronic communication" means "any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photo-optical system." La. R.S. 15:1302(8)(a).

191.

Defendant aided in, and continues to aid in, the interception of contents in that the data from the electronic communications between Plaintiff and/or Class Members and Defendant that were redirected to and recorded by the third parties include information which identifies the parties to each communication, their existence, and their contents.

192.

Defendant aided in the interception of "contents" in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. Personally identifying information such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of patient communications about specific treatments;

g. The precise text of patient communications about scheduling appointments with medical providers;

h. The precise text of patient communications about billing and payment;

i. The precise text of specific buttons on Defendant's website(s) that patients click to exchange communications, including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

j. The precise dates and times when patients click to Log-In on Defendant's website(s);

k. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information; and

l. Any other content that Defendant has aided third parties in scraping from webpages or communication forms at web properties.

193.

Plaintiff and Class Members reasonably expected that their Personal Health Information was not being contemporaneously intercepted, recorded, and disclosed to Facebook and other third parties.

194.

Neither Plaintiff nor Class Members consented to the disclosure of their Personal Health Information by Defendant to Facebook and other third parties. Nor could they have consented, given that Defendant never sought Plaintiff's or Class Members' consent.

195.

Plaintiff's and Class Members' electronic communications were intercepted during transmission, without their consent. Defendant undertook each such interception for numerous criminal and/or tortious purposes, and for the purpose of committing injurious act(s), at the time of each such interception by Defendant. Defendant's criminal and/or tortious purposes, and its intended injurious act(s), include (but not limited to) those specified below.

196.

For example, Defendant intercepted Plaintiff and Class Members' electronic communications for the purpose of disclosing those communications, including Plaintiff's and Class Members' Personal Health Information contained in those communications, to Facebook and other third parties without the knowledge, consent, or written authorization of Plaintiff or Class Members. Because the disclosure of Plaintiff's and Class Members' Personal Health Information without consent or proper authorization is both a criminal and tortious act that

violates multiple laws, including (but not limited to) 48 La. Admin. Code Pt. 1, §9319(14), 48 La. Admin. Code Pt. 1, § 505, La. Stat. § 40:1173.1, La. Stat. § 40:1173.6, La. Rev. Stat. § 13:3715.1, and La. Rev. Stat. § 51:3074, as well as Louisiana Civil Code Articles 2315, 2316 and/or 2324(A), Defendant's misconduct falls within the ambit of Louisiana's wiretapping statute. Intentionally committing such criminal and/or tortious disclosures of Plaintiff's and Class Members' Personal Health Information in violation of the Louisiana Wiretapping Act also show Defendant's purpose of committing injurious acts to Plaintiffs and Class Members at the time of each interception.

197.

Likewise, at the time Defendant intentionally intercepted Plaintiff's and Class Members' electronic communications, Defendant did so with the purpose of willfully disclosing Plaintiffs' and Class Members' Personal Health Information to Facebook, while knowing or at least having reason to know such communications and Personal Health Information were obtained illegally in violation of the Louisiana Wiretapping Statute. This illicit purpose is a separate criminal and tortious act that is specifically prohibited by Louisiana law. La. R.S. 15.1303(3).

198.

In addition, at the time Defendant intentionally intercepted Plaintiff's and Class Members' electronic, Defendant also did so with the purpose of using those communications to barter Plaintiff's and Class Members' Personal Health Information in return for access to Facebook's Meta Pixel tool. Because "willfully us[ing]" the contents of Plaintiff's and Class Members' electronic communications to obtain access to Facebook's Meta Pixel tool—when Defendant knew or had reason to know that these communications were obtained illegally—is a separate criminal and tortious act in violation of La. R.S. 15:1303:(4), Defendant's misconduct falls within the ambit of the Louisiana Wiretapping Statute for this additional reason as well.

199.

Further, at the time Defendant intentionally intercepted Plaintiff's and Class Members' electronic communications, Defendant did so with the purpose of committing further criminal, tortious, and/or injurious acts against Plaintiffs and Class Members by misappropriating Plaintiff's

and Class Members' Personal Health Information so that Defendant could monetize and exploit that information without paying fair value for such valuable information.

200.

Defendant's interception of Plaintiff's and Class Members' electronic communications for the purpose of bartering, selling, or otherwise providing their Personal Health Information to Facebook in return for access to Facebook's Meta Pixel tool is tortious under Louisiana Civil Code Articles 2315, 2316 and/or 2324(A). (*see also, e.g.,* La. Civ. Code art. 2930) For example, and without limitation, such conduct constitutes the tort of conversion under Louisiana law, which is committed when any of the following occurs: 1) possession is acquired in an unauthorized manner; 2) the chattel is removed from one place to another with the intent to exercise control over it; 3) possession of the chattel is transferred without authority; 4) possession is withheld from the owner or possessor; 5) the chattel is altered or destroyed; 6) the chattel is used improperly; or 7) ownership is asserted over the chattel. Defendant's interception of Plaintiff's and Class Members' electronic communications for the purpose bartering and/or selling that information to Facebook constitutes tortious and/or injurious acts of conversion against Plaintiffs and Class Members at least because (1) Defendant has acquired possession of the Personal Health Information in an unauthorized manner (*i.e.*, electronic interception without consent), (2) Defendant has removed such Personal Health Information from Plaintiff's and Class Members' possession to its own (via electronic interception) with the intent to exercise control over that information (*i.e.*, for disclosure to Facebook), (3) Defendant has transferred the Personal Health Information intercepted (including to Facebook) without authorization from Plaintiff or Class Members, or (4) Defendant has improperly used the intercepted communications to transfer Personal Health Information contained or reflected therein to Facebook.

201.

By disclosing Plaintiff's and Class Members' Personal Health Information to Facebook without their knowledge or consent, Defendant deprived Plaintiff and Class Members of their property rights in their Personal Health Information and caused Plaintiff and Class Members injury by (1) diminishing the value of their Personal Health Information, (2) depriving Plaintiff and Class Members of the full value of the medical services for which they paid, which included Defendant's obligation to maintain the confidentiality of their Personal Health Information, and (3) depriving Plaintiffs and Class Members of their right to control who had access to their sensitive medical

and personal information. Defendant's decision to steal and exploit Plaintiff's and Class Members' Personal Health Information without their knowledge or consent is sufficient to bring Defendant's conduct within the ambit of Louisiana's wiretapping statute.

202.

Under the Louisiana Wiretapping Act, aggrieved persons are entitled to recover appropriate injunctive relief and "(1) actual damages, but not less than liquidated damages computed at the rate of $100 per day for each day of violation or one thousand dollars, whichever is greater" (2) "a reasonable attorney's fee and other litigation costs reasonably incurred" and (3) "Punitive Damages." La. R.S. 15:1312.

203.

In addition to statutory damages, Defendant's conduct caused Plaintiff and Class Members the following damages:

a. Sensitive and confidential information that Plaintiff and Class Members intended to remain private is no longer private;

b. Defendant eroded the essential confidential nature of the doctor-patient relationship;

c. Defendant took something of value from Plaintiff and Class Members and derived benefit therefrom without Plaintiff's and Class Members' knowledge or informed consent and without sharing the benefit of such value; and

d. Defendant's actions diminished the value of Plaintiff's and Class Members' personal information.

COUNT II
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

204.

Plaintiff re-alleges and incorporates by reference all paragraphs above as if fully set forth herein.

205.

Plaintiff brings this claim on behalf of herself and all members of the Class.

206.

Plaintiff and Class Members conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private. Defendant collected, used, and disclosed this information for its own gain, including for advertisement purposes, sale, or trade for valuable

services from third parties. Additionally, Plaintiff and the Class Members conferred a benefit on Defendant in the form of monetary compensation.

207.

Plaintiff and the Class Members would not have used the Defendant's services, or would have paid less for those services, if they had known that Defendant would collect, use, and disclose this information to third parties. Defendant's disclosure of Plaintiff's and Class Member's Personal Health Information to third parties including Facebook resulted in an impoverishment to Plaintiff and Class Members by diminishing the value of Plaintiff's and Class Members' Personal Health Information. There is a direct connection between Defendant's unjust enrichment and the resulting impoverishment suffered by Plaintiff and Class Members.

208.

Defendant unjustly retained those benefits at the expense of Plaintiff and Class Members because Defendant's conduct damaged Plaintiff and Class Members, all without providing any commensurate compensation to Plaintiff and Class Members. There is no justification for Defendant's disclosure of Plaintiff's and Class Member's Personal Health Information to Facebook and other third parties.

209.

The benefits that Defendant derived from Plaintiff and Class Members rightly belong to Plaintiff and Class Members. It would be inequitable under unjust enrichment principles for Defendant to be permitted to retain any of the profit or other benefits it derived from the unfair and unconscionable methods, acts, and trade practices alleged in this Complaint.

210.

Defendant should therefore be compelled to disgorge in a common fund for the benefit of Plaintiff and Class Members all unlawful or inequitable proceeds that Defendant received, and should be enjoined from engaging in further unlawful and inequitable conduct, as described herein.

PRAYER FOR RELIEF

WHEREFORE Plaintiff respectfully prays that this Petition be deemed good and sufficient; that, after due proceedings be had, this action be certified as a class action pursuant to Articles 591(B)(2) and /or (B)(3) of the Louisiana Code of Civil Procedure; and that, after further proceedings be had, there be judgment in favor of Plaintiff and the proposed class and against Defendant for all damages and other remedies together with the costs of these proceedings, legal

interest, attorney's fees, and any and all general or equitable relief, including injunctive relief, which may be reasonable under the circumstances.

Respectfully submitted,

/s/ Stephen J. Herman
Stephen J. Herman, La. Bar No. 23129
Joseph E. "Jed" Cain, La. Bar No. 29785
HERMAN, HERMAN, & KATZ, LLC
820 O'Keefe Avenue
New Orleans, Louisiana 70113
Telephone: (504) 581-4892
Facsimile: (504) 561-6024
E-Mail: sherman@hhklawfirm.com
E-Mail: jcain@hhklawfirm.com

Foster C. Johnson (*pro hac vice forthcoming*)
David Warden (*pro hac vice forthcoming*)
Weining Bai (*pro hac vice forthcoming*)
AHMAD, ZAVITSANOS, & MENSING, P.C.
1221 McKinney Street, Suite 3460
Houston, Texas 77010
Telephone: (713) 655-1101
E-Mail: fjohnson@azalaw.com
E-Mail: dwarden@azalaw.com
E-Mail: wbai@azalaw.com

Keenan K. Kelly, La. Bar No. 22477
William L. Townsend, III, La. Bar No.17837
KELLY & TOWNSEND, LLC
137 Saint Denis Street
Natchitoches, Louisiana 71457
Telephone: (318)352-2353
Facsimile: (318)352-8918
E-Mail: keenan@keltownlaw.com
E-Mail: billt@keltownlaw.com

Counsel for Plaintiff, Jacqueline Horton, Individually and on Behalf of All Others Similarly Situated

PLEASE SERVE:
Petition, together with:
Requests for Admissions, Interrogatories, and
Requests for Production, on:

WILLIS-KNIGHTON MEDICAL CENTER.
Through its Designated Agent for Service of Process:
Lamar P. Pugh
333 Texas Street, STE 2100,
Shreveport, LA 71101